IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No.: 3018
BELANGER *et al.*	Art Unit: 2436
Appl. No.: 10/659,368	Examiner: Johnson, Carlton
Filed: September 11, 2003	Atty. Docket: 2222.3810000
For: **System and Method for Data Access and Control**	

RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF

Mail Stop Appeal Brief - Patents

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In reply to the Notification of Non-Compliant Appeal Brief dated June 16, 2011, Appellants submit the following revised Summary of Claimed Subject Matter and Claims Appendix. It is not believed that extensions of time are required beyond those that may otherwise be provided for in documents accompanying this paper. However, if additional extensions of time are necessary to prevent abandonment of this application, then such extensions of time are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required therefor (including fees for net addition of claims) are hereby authorized to be charged to our Deposit Account No. 19-0036.

In accordance with M.P.E.P. § 1205.03(B) and the Notice of Non-Compliant Appeal Brief dated June 16, 2011, only a revised copy of the Summary of Claimed Subject Matter and Claims Appendix are provided herein, numbered in accordance with the sections' positions in the Appeal Brief of June 6, 2011.

V. Summary of Recited Subject Matter (37 C.F.R. § 41.37(c)(1)(v))

A concise explanation of the subject matter recited in each of the independent claims on appeal (i.e., claims 1, 7, 15, 16, 23, 24, 29, and 30) is provided below. The explanation refers to the specification by page and line number and to the drawings by reference characters. Reference is made to example supporting embodiments disclosed in the specification, although it is understood that the claims should not be limited to the specific embodiments to which reference is made.

Each independent claim involved in the appeal, and every means plus function and step plus function as permitted by 35 U.S.C. § 112, sixth paragraph, are identified. Example structure, material, or acts described in the specification as corresponding to each recited function are set forth with reference to the specification by page and line number, and to the drawings, if any, by reference characters.

A. Independent Claim 1

Claim 1 recites a method that comprises:

- receiving, using a processing device, a first request, from a first sponsor of an access candidate, for access to a first security level in a computer network, wherein the first security level secures computational resources for accessing electronic data (e.g., Pg. 6, Lns. 24-25; Pg. 8, Lns. 19-27);

- determining, using the processing device, whether access candidate attributes satisfy access requirements of the resources (e.g., Pg. 6, Lns. 25-26; Pg. 9, Lns. 1-20), wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first level is prohibited (e.g., Pg. 9, Lns. 23-30; Pg. 11, Ln. 29 - Pg. 12, Ln. 2);

- granting, using the processing device, access to the first security level based on a determination indicating that access to the first level is not prohibited (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 1-6);

- receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to a second security level in the computer network in response to the granting of access to the first security level, wherein the second security level secures the electronic data (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 10-11 and Lns. 24-30);

- determining, using the processing device, whether the access candidate attributes satisfy access requirements of the electronic data (e.g., Pg. 6, Ln. 28 - Pg. 7, Ln 3; Pg. 11, Lns. 1-5 and Lns. 15-19);

- obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy the access requirements of the electronic data in response to a determination indicating that access to the second security level is prohibited (e.g., Pg. 7, Lns. 2-5; Pg. 11, Lns. 20-28); and

- in response to obtaining the authorization from the resolution authority, granting access to the second security level (e.g., Pg. 11, Lns. 25-28; Pg. 16, Lns.4-14).

B. Independent Claim 7

Claim 7 recites a method that comprises:

- receiving, using a processing device, a first request, from a first sponsor of an access candidate, for physical access to a computer network (e.g., Pg. 6, Lns. 24-25; Pg. 8, Lns. 19-27);

- determining, using the processing device, whether access candidate attributes satisfy access requirements of physical access, (e.g., Pg. 6, Lns. 25-26; Pg. 9, Lns. 1-20), wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that physical access is prohibited (e.g., Pg. 9, Lns. 23-30; Pg. 11, Ln. 29 - Pg. 12, Ln. 2);

- granting, using the processing device, the physical access to the computer network based on a determination indicating that physical access is not prohibited (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 1-6);

- receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to electronic data in the computer network in response to the granting of physical access to the computer network (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 10-11 and Lns. 24-30);

- determining, using the processing device, whether the access candidate attributes satisfy access requirements of the electronic data (e.g., Pg. 6, Ln. 28 - Pg. 7, Ln 3; Pg. 11, Lns. 1-5 and Lns. 15-19);

- obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy access requirements of the electronic data in response to a determination indicating that access to the electronic data is prohibited (e.g., Pg. 7, Lns. 2-5; Pg. 11, Lns. 20-28); and

- in response to obtaining the authorization from the resolution authority, granting access to the electronic data (e.g., Pg. 11, Lns. 25-28; Pg. 16, Lns.4-14).

C. Independent Claim 15

Claim 15 recites a method that comprises:

- identifying, using a processing device, a plurality of data subsets of electronic data, wherein respective data subsets correspond to respective sets of access requirements (e.g., Pg. 12, Lns. 12-21);

- determining, using the processing device, at least one data class associated with the respective data subsets, the at least one data class identifying at least a citizenship requirement and a location requirement for access to data associated with the at least one data class (e.g., Pg. 12, Lns. 21-27; Pg. 17, Ln. 30 - Pg. 18, Ln 6);

- receiving, using the processing device, a first request, from a first sponsor of an access candidate, for access to a first security level in a computer network, wherein the first security level secures physical access to a computer workstation for accessing the electronic data, the first request including access attributes of the access candidate (e.g., Pg. 6, Lns. 24-25; Pg. 8, Lns. 19-27) comprising an indication of a citizenship status of the access candidate, an indication of a current location of the access candidate, and an indication of an existence of a data access agreement with the access candidate (e.g., Pg. 9, Lns. 5-12; Pg. 16, Lns. 24-26);

- determining, using the processing device, whether the access candidate attributes satisfy access requirements of the first security level, wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first security level is prohibited (e.g., Pg. 9, Lns. 23-30; Pg. 11, Ln. 29 - Pg. 12, Ln. 2);

- granting, using the processing device, access to the first security level based on a determination indicating that access to the first security level is not prohibited (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 1-6);

- receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to a second security level in the computer network in response to the granting of access to the first security level, wherein the second security level secures access to at least one of the plurality of data subsets (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 10-11 and Lns. 24-30);

- determining, using the processing device, whether the access candidate attributes satisfy the respective set of access requirements corresponding to the at least one of the plurality of data subsets (e.g., Pg. 6, Ln. 28 - Pg. 7, Ln 3; Pg. 11, Lns. 1-5 and Lns. 15-19);

- obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy the respective set of access requirements corresponding to the at least one of the plurality of data subsets in response to a determination indicating that access to the at least one of the plurality of data subsets is prohibited (e.g., Pg. 7, Lns. 2-5; Pg. 11, Lns. 20-28); and

- in response to obtaining the authorization from the resolution authority, granting access to the second security level (e.g., Pg. 11, Lns. 25-28; Pg. 16, Lns.4-14).

D. Independent Claim 16

Claim 16 recites a system that comprises:

- storage means for receiving and storing (e.g., Pg. 7, Lns. 14-16; FIG.1, elements 134, 138, 140, 142) electronic data using a computer network (e.g., Pg. 7, Lns. 11-13 and Lns. 14-16);

- means for evaluating (e.g., Pg. 7, Ln. 29 - Pg. 8, Ln 9; FIG.1, element 104; FIG. 2, element 208) a first request for access to one or more resources in the computer network, wherein the resources secure the electronic data, wherein an evaluation of the first request includes a first comparison of one or more attributes of the access candidate with one or more access requirements associated with the resources (e.g., Pg. 6, Lns. 24-25; Pg. 8, Ln. 19 - Pg. 9, Ln. 20), and wherein the one or more attributes of the access candidate are revisable if the first comparison indicates that access is prohibited (e.g., Pg. 9, Lns. 23-30; Pg. 11, Ln. 29 - Pg. 12, Ln. 2);

- means for granting access (e.g., Pg. 10, Lns. 1-3; FIG. 1, element 104; FIG. 2, element 208) to the one or more resources if the first comparison indicates that access is not prohibited (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 1-6);

- means for evaluating (e.g., Pg. 10, Lns. 10-11; FIG. 1, element 106; FIG. 3, elements 306 and 308) a second request for access to the electronic data by the one or more resources, wherein an evaluation of the second request includes a second comparison of the one or more attributes of the access candidate with one or more access requirements associated with the electronic data (e.g., Pg. 6, Ln. 27 - Pg. 7, Ln 3; Pg. 10, Lns. 10-11 and Lns. 24-30; Pg. 11, Lns. 1-5 and Lns. 15-19);

- means for obtaining authorization (e.g., Pg. 11, Lns. 20-22; FIG. 1, element 106; FIG. 3, elements 306 and 308) for the second request form a resolution authority (e.g., Pg. 11, Lns. 20-22; FIG. 1, element 124; FIG. 3, element 320) if the one or more attributes of the access candidate fails to satisfy one or more access requirements associated with the electronic data in response to the evaluation of the second request indicating that access to the electronic data is prohibited (e.g., Pg. 7, Lns. 2-5; Pg. 11, Lns. 20-28; Pg. 15, Lns. 24-30); and

- means for granting (e.g., Pg. 11, Lns. 25-28; element 106; FIG. 3, elements 306 and 308), in response to obtaining the authorization from the resolution authority, the access candidate access to the electronic data using the one or more resources (e.g., Pg. 11, Lns. 25-28; Pg. 16, Lns.4-14).

E. *Independent Claim 23*

Claim 23 recites a system that comprises:

- storage (e.g., Pg. 7, Lns. 14-16; FIG.1, elements 134, 138, 140, 142) configured to receive and store electronic data using a computer network (e.g., Pg. 7, Lns. 11-13 and Lns. 14-16);

- one or more resources configured to process and manipulate the electronic data using a computer network (e.g., Pg. 6, Lns. 21-25; Pg. 8, Lns. 3-9; FIG.1, element 110);

- a resource access controller (e.g., Pg. 7, Ln. 29 - Pg. 8, Ln 9; FIG.1, element 104; FIG. 2, element 208) configured to grant access to one or more resources, in response to a request for access to the one or more resources (e.g., Pg. 6, Lns. 24-25; Pg. 8, Ln. 19 - Pg. 9, Ln. 20), based at least in part on a comparison of a citizenship status and a current location of an access candidate and an existence of a data access agreement with a citizenship requirement, wherein the location requirement and the data access agreement requirement are associated with the one or more resources (e.g., Pg. 6, Lns. 27-28; Pg. 9, Lns. 5-12; Pg. 10, Lns. 1-6; Pg. 16, Lns. 24-26);

- one or more data access controllers (e.g., Pg. 10, Lns. 10-11; FIG. 1, element 106; FIG. 3, elements 306 and 308) configured to grant access to a corresponding portion of the electronic data based at least in part on a comparison of the citizenship status and the current location of the access candidate with the citizenship requirement and the location requirement associated with the one or more data classes of the corresponding portion of the electronic data (e.g., Pg. 6, Ln. 27 - Pg. 7, Ln 3; Pg. 10, Lns. 10-11 and Lns. 24-30; Pg. 11, Lns. 1-5 and Lns. 15-19);

- one or more resolution authorities to (e.g., Pg. 11, Lns. 20-22; FIG. 1, element 124; FIG. 3, element 320) configured to:

- modify access requirements associated with the one or more data classes (e.g., Pg. 11, Lns. 25-28), and

- authorize access to one or more portions of the electronic data in response to a comparison performed by a corresponding data access controller indicating that access is prohibited (e.g., Pg. 11, Ln. 20 - Pg. 12, Ln. 2; Pg. 15, Ln. 24 - Pg. 16, Ln. 9); and

- a data access module (e.g., Pg. 12, Lns. 12-27; FIG. 1, element 106; FIG. 3, elements 306 and 308) configured to:
- evaluate a request for access to one or more portions of the electronic data using the one or more resources (e.g., Pg. 12, Lns. 21-27),
- identify one or more data access controllers corresponding to the one or more portions of the electronic data (e.g., Pg. 12, Lns. 12-21), and
- forward the request for access to the one or more identified data access controllers for evaluation regarding whether to grant access to the corresponding one or more portions of the electronic data (e.g., Pg. 15, Ln. 24 - Pg. 16, Ln. 14).

F. Independent Claim 24

Claim 24 recites a method that comprises:

- receiving, using a controller in a computer network associated with secured electronic data, a request for access to secured electronic data in the computer network (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 10-11 and Lns. 24-30);
- comparing, using the controller, one or more attributes of an access candidate with one or more access requirements associated with the secured electronic data (e.g., Pg. 6, Ln. 28 - Pg. 7, Ln 3; Pg. 11, Lns. 1-5 and Lns. 15-19);

- obtaining authorization for the request from a resolution authority if one or more attributes of the access candidate fails to satisfy one or more access requirements associated with the secured electronic data (e.g., Pg. 7, Lns. 2-5; Pg. 11, Ln. 20-28; Pg. 15, Lns. 24-30); and

- in response to obtaining or not obtaining authorization from the resolution authority, granting or denying in whole or in part, using the controller, access to the secured electronic data based, at least in part, on a determination based on access candidate information and request related information (e.g., Pg. 11, Ln. 25 - Pg. 12, Ln. 11; Pg. 16, Lns.4-14),

- wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination denying access to the secured electronic data (e.g., Pg. 9, Lns. 23-30; Pg. 11, Ln. 29 - Pg. 12, Ln. 2).

G. Independent Claim 29

Claim 29 recites a method that comprises:

- receiving, using a controller in a computer network associated with secured electronic data in the computer network, a request for access to the secured electronic data in the computer network (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 10-11 and Lns. 24-30);

- comparing, using the controller, one or more attributes of an access candidate with one or more access requirements associated with the secured electronic data (e.g., Pg. 6, Ln. 28 - Pg. 7, Ln 3; Pg. 11, Lns. 1-5 and Lns. 15-19);

- granting, using the controller, access to the secured electronic data in response to a comparison indicating that access by the access candidate is not prohibited (e.g., Pg. 7, Ln. 28 - Pg. 7, Ln. 1; Pg. 10, Lns 24-30; Pg. 12, Ln. 3-11);

- obtaining authorization for the request from a resolution authority in response to a comparison indicating that access by the access candidate is prohibited (e.g., Pg. 7, Lns. 2-5; Pg. 11, Ln. 20-28; Pg. 15, Lns. 24-30);

- in response to obtaining or not obtaining authorization from the resolution authority, granting or denying in whole or in part, using the controller access to the secured electronic data based, at least in part, on a determination based on access candidate information and request related information (e.g., Pg. 11, Ln. 25 - Pg. 12, Ln. 11; Pg. 16, Lns.4-14),

- wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination denying access to the secured electronic data (e.g., Pg. 9, Lns. 23-30; Pg. 11, Ln. 29 - Pg. 12, Ln. 2).

H. Independent Claim 30

Claim 30 recites an article of manufacture including a non-transitory computer-readable medium (e.g., FIG. 1, elements 104 and 106; Pg. 18, Lns. 7-11) having instructions stored thereon, execution of which causes a processing device to perform operations comprising:

- receiving, using a processing device, a request for access to a first security level in a computer network (e.g., Pg. 6, Lns. 24-25; Pg. 8, Lns. 19-27);

- comparing, using the processing device, one or more attributes of an access candidate with one or more access requirements associated with the first security level, (e.g., Pg. 6, Lns. 25-26; Pg. 9, Lns. 1-20), wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination indicating that access by the access candidate to the first security level is prohibited (e.g., Pg. 9, Lns. 23-30; Pg. 11, Ln. 29 - Pg. 12, Ln. 2);

- granting, using the processing device, access to the first security level based on a comparison indicating that access by the access candidate to the first security level is not prohibited (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 1-6);

- receiving, using the processing device, a request for access to a second security level in the computer network (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 10-11 and Lns. 24-30);

- obtaining authorization for the request from a resolution authority in response to a comparison indicating that access by the access candidate is prohibited (e.g., Pg. 7, Lns. 2-5; Pg. 11, Lns. 20-28).

Each of independent claims 1, 7, 15, 16, 23, 24, 29, and 30 finds support ***at least*** in the above-referenced sections of the Specification. The remaining claims draw support from the aforementioned sections of the Specification.

VIII. Claims Appendix (37 C.F.R. § 41.37(c)(1)(viii))

1. A method comprising:

receiving, using a processing device, a first request, from a first sponsor of an access candidate, for access to a first security level in a computer network, wherein the first security level secures computational resources for accessing electronic data;

determining, using the processing device, whether access candidate attributes satisfy access requirements of the resources, wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first level is prohibited;

granting, using the processing device, access to the first security level based on a determination indicating that access to the first level is not prohibited;

receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to a second security level in the computer network in response to the granting of access to the first security level, wherein the second security level secures the electronic data;

determining, using the processing device, whether the access candidate attributes satisfy access requirements of the electronic data secured by the second security level;

obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy the access requirements of the electronic data in response to a determination indicating that access to the second security level is prohibited; and

in response to obtaining the authorization from the resolution authority, granting the access candidate access to the second security level.

2. The method of Claim 1, further comprising granting access to the second security level in response to determining that the access candidate attributes satisfy the access requirements of the electronic data.

3. The method of Claim 1, further comprising denying access to the second security level if the authorization for the second request cannot be obtained.

4. The method of Claim 1, wherein at least one of the access requirements of the resources and the access requirements of the electronic data are represented as part of a graphical display associated with the access candidate and accessed for display to a controller via a network.

5. The method of Claim 1, wherein at least one of the access requirements of the resource and the access requirements of the electronic data comprise a citizenship status of the access candidate or a current location of the access candidate.

6. The method of Claim 5, wherein the access candidate attributes comprise a citizenship status of the access candidate or a current location of the access candidate.

7. A method comprising:

receiving, using a processing device, a first request, from a first sponsor of an access candidate, for physical access to a computer network;

determining, using the processing device, whether access candidate attributes satisfy access requirements of physical access, wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that physical access is prohibited;

granting, using the processing device, the physical access to the computer network based on a determination indicating that physical access is not prohibited;

receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to electronic data in the computer network in response to the granting of physical access to the computer network;

determining, using the processing device, whether the access candidate attributes satisfy access requirements of the electronic data;

obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy access requirements of the electronic data in response to a determination indicating that access to the electronic data is prohibited; and

in response to obtaining the authorization from the resolution authority, granting the access candidate access to the electronic data.

8. The method of Claim 7, further comprising granting access to the electronic data in response to a comparison of the access candidate attributes with the access requirements of the electronic data indicating that access to the electronic data is not prohibited.

9. The method of Claim 7, further comprising denying access to the electronic data if the authorization for the second request cannot be obtained.

10. The method of Claim 7, wherein the access candidate attributes are represented as part of a graphical display associated with the access candidate and accessed for display via a network.

11. The method of Claim 7, wherein at least one of the access requirements of the electronic data and the access requirements of physical access comprise a valid data access agreement with the access candidate; a current location of the access candidate; or a citizenship status of the access candidate.

12. The method of Claim 11, wherein the access candidate attributes comprise an existence of a data access agreement; a current location of the access candidate; or a citizenship status of the access candidate.

13. The method as in Claim 7, wherein at least one of the access requirements of the electronic data and access requirements of physical access comprise a current location of the access candidate or a citizenship status of the access candidate.

14. The method of Claim 7, wherein at least one of the request for physical access or the request for access to the electronic data is submitted by more than one sponsor of the access candidate.

15. A method comprising:

identifying, using a processing device, a plurality of data subsets of electronic data, wherein respective data subsets correspond to respective sets of access requirements;

determining, using the processing device, at least one data class associated with the respective data subsets, the at least one data class identifying at least a citizenship requirement and a location requirement for access to data associated with the at least one data class;

receiving, using the processing device, a first request, from a first sponsor of an access candidate, for access to a first security level in a computer network, wherein the first security level secures physical access to a computer workstation for accessing the electronic data, the first request including access attributes of the access candidate comprising an indication of a citizenship status of the access candidate, an indication of a current location of the access candidate, and an indication of an existence of a data access agreement with the access candidate;

determining, using the processing device, whether the access candidate attributes satisfy access requirements of the first security level, wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first security level is prohibited;

granting, using the processing device, access to the first security level based on a determination indicating that access to the first security level is not prohibited;

receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to a second security level in the computer network in response to the granting of access to the first security level, wherein the second security level secures access to at least one of the plurality of data subsets;

determining, using the processing device, whether the access candidate attributes satisfy the respective set of access requirements corresponding to the at least one of the plurality of data subsets;

obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy the respective set of access requirements corresponding to the at least one of the plurality of data subsets in response to a determination indicating that access to the at least one of the plurality of data subsets is prohibited; and

in response to obtaining the authorization from the resolution authority, granting the access candidate access to the second security level.

16. A system comprising:

storage means for receiving and storing electronic data using a computer network;

means for evaluating a first request for access to one or more resources in the computer network, wherein the resources secure the electronic data, wherein an evaluation of the first request includes a first comparison of one or more attributes of the access candidate with one or more access requirements associated with the resources, and wherein the one or more attributes of the access candidate are revisable if the first comparison indicates that access is prohibited;

means for granting access to the one or more resources if the first comparison indicates that access is not prohibited;

means for evaluating a second request for access to the electronic data by the one or more resources, wherein an evaluation of the second request includes a second comparison of the one or more attributes of the access candidate with one or more access requirements associated with the electronic data;

means for obtaining authorization for the second request form a resolution authority if the one or more attributes of the access candidate fails to satisfy one or more access requirements associated with the electronic data in response to the evaluation of the second request indicating that access to the electronic data is prohibited; and

means for granting, in response to obtaining the authorization from the resolution authority, the access candidate access to the electronic data using the one or more resources.

17. The system of Claim 16, further comprising means for granting access to the electronic data using the one or more resources configured to access and manipulate the electronic data if the second comparison indicates that access to the electronic data is not prohibited.

18. The system of Claim 16, wherein the access candidate is denied access to the electronic data if the authorization for the second request cannot be obtained.

19. The system of Claim 16, wherein the one or more access candidate attributes are represented as part of a graphical display associated with the access candidate and accessed for display via a network.

20. The system of Claim 16, wherein at least one of the one or more access requirements associated with the recourses and the one or more access requirements associated with the electronic data relates to at least one of: a valid data access agreement with a potential access candidate; a current location of the potential access candidate; or a citizenship status of the potential access candidate.

21. The system of Claim 20, wherein the one or more access candidate attributes relates to at least one of: an indication an existence of a data access agreement with the access candidate; a current location of the access candidate; or a citizenship status of the access candidate.

22. The system of Claim 16, wherein the one or more access requirements associated with the electronic data includes at least one of a current location of the access candidate or a citizenship status of the access candidate.

23. A system comprising:

storage configured to receive and store electronic data using a computer network;

one or more resources configured to process and manipulate the electronic data using a computer network;

a resource access controller configured to grant access to one or more resources, in response to a request for access to the one or more resources, based at least in part on a comparison of a citizenship status and a current location of an access candidate and an existence of a data access agreement with a citizenship requirement, wherein the location requirement and the data access agreement requirement are associated with the one or more resources;

one or more data access controllers configured to grant access to a corresponding portion of the electronic data based at least in part on a comparison of the citizenship status and the current location of the access candidate with the citizenship requirement and the location requirement associated with the one or more data classes of the corresponding portion of the electronic data;

one or more resolution authorities configured to:

modify access requirements associated with the one or more data classes, and

authorize access to one or more portions of the electronic data in response to a comparison performed by a corresponding data access controller indicating that access is prohibited; and

a data access module configured to:

evaluate a request for access to one or more portions of the electronic data using the one or more resources,

identify one or more data access controllers corresponding to the one or more portions of the electronic data, and

forward the request for access to the one or more identified data access controllers for evaluation regarding whether to grant access to the corresponding one or more portions of the electronic data.

24. A method comprising:

receiving, using a controller in a computer network associated with secured electronic data, a request for access to the secured electronic data in the computer network;

comparing, using the controller, one or more attributes of an access candidate with one or more access requirements associated with the secured electronic data;

obtaining authorization for the request from a resolution authority if one or more attributes of the access candidate fails to satisfy one or more access requirements associated with the secured electronic data; and

in response to obtaining or not obtaining authorization from the resolution authority, granting or denying in whole or in part, using the controller, access to the secured electronic data based, at least in part, on a determination based on access candidate information and request related information,

wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination denying access to the secured electronic data.

25. The method of Claim 24, further comprising granting access to the secured electronic data in response to a comparison indicating that access by the access candidate is not prohibited.

26. The method of Claim 24, wherein the one or more access requirements associated with the secured electronic data are represented as part of a graphical display associated with the access candidate and accessed for display to the controller via a network.

27. The method of Claim 24, wherein the one or more access requirements associated with the secured electronic data are related to at least one of a citizenship status or a current location of the access candidate.

28. The method of Claim 27, wherein the one or more attributes of the access candidate include at least one of a citizenship status or a current location of the access candidate.

29. A method comprising:

receiving, using a controller in a computer network associated with secured electronic data in the computer network, a request for access to the secured electronic data in the computer network;

comparing, using the controller, one or more attributes of an access candidate with one or more access requirements associated with the secured electronic data;

granting, using the controller, access to the secured electronic data in response to a comparison indicating that access by the access candidate is not prohibited;

obtaining authorization for the request from a resolution authority in response to a comparison indicating that access by the access candidate is prohibited; and

in response to obtaining or not obtaining authorization from the resolution authority, granting or denying in whole or in part, using the controller, access to the secured electronic data based, at least in part, on a determination based on access candidate information and request related information,

wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination denying access to the secured electronic data.

30. An article of manufacture including a non-transitory computer-readable medium having instructions stored thereon, execution of which causes a processing device to perform operations comprising:

receiving, using a processing device, a request for access to a first security level in a computer network;

comparing, using the processing device, one or more attributes of an access candidate with one or more access requirements associated with the first security level, wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination indicating that access by the access candidate to the first security level is prohibited;

granting, using the processing device, access to the first security level based on a comparison indicating that access by the access candidate to the first security level is not prohibited;

receiving, using the processing device, a request for access to a second security level in the computer network;

obtaining authorization for the request from a resolution authority in response to a comparison indicating that access by the access candidate is prohibited.

31. The article of manufacture of Claim 30, further comprising granting access to the second security level in response to a comparison of the one or more attributes of the access candidate with the one or more access requirements associated with the second security level indicating that access to the second security level by the access candidate is not prohibited.

32. The article of manufacture of Claim 30, further comprising denying access to the second security level if the authorization for the request cannot be obtained.

33. The article of manufacture of Claim 30, wherein the one or more attributes of the access candidate is represented as part of a graphical display associated with the access candidate and accessed for display via a network.

34. The article of manufacture of Claim 30, wherein the one or more access requirements associated with the first security level relates to at least one of: a valid data access agreement with the access candidate; a current location of the access candidate; or a citizenship status of the access candidate.

35. The article of manufacture of Claim 34, wherein the one or more attributes of the access candidate relates to at least one of: an indication of whether the access candidate has a data access agreement; a current location of the access candidate; or a citizenship status of the access candidate.

36. The article of manufacture of Claim 30, wherein the one or more access requirements associated with the second security level relates to at least one of a current location of the access candidate or a citizenship status of the access candidate.

37. The article of manufacture of Claim 30, wherein at least one of the request for access to the first security level or the request for access to the second security level is submitted by one or more sponsors.

38. The method as in claim 1, further comprising granting a waiver of the access requirements.

39. (Cancelled)

40. (Cancelled)

41. The method of claim 1, further comprising receiving supplemental evidence verifying the access candidate attributes.

42. The system of claim 15, wherein the data subsets are separated into the at least one data class based on a data provider of the data.

43. The method of claim 15, wherein the physical access comprises physical access to a facility housing the computer workstation.

44. The method of claim 15, wherein the physical access comprises logging on to the computer workstation.

Conclusion

Prompt and favorable consideration of this Response to Notification of Non-Compliant Appeal Brief is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Glenn J. Perry
Attorney for Applicants
Registration No. 28,458

Date: 11 July 2011

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600
1382595_1.DOC